Available online at www.sciencedirect.com

ScienceDirect

Procedia Engineering 128 (2015) 74 – 82

Procedia Engineering

www.elsevier.com/locate/procedia

3rd European STAMP Workshop, STAMP EU 2015

System theoretic approaches in the process industries

Simon Lucchini[a], Stephen Johnson[a,*]

[a]*Fluor Canada Ltd. 55Sunpark Plaza SE, Calgary, Canada T2X 1K1*

Abstract

The world of the energy & chemicals industry has been slow to adopt systems theoretic approaches. The focus of this paper is a summary of the present state of the industry in terms of technical design HSE practice – the world of process safety. This will then be followed by some consideration of the barriers to adoption of more rigorous systems theoretic type approaches, and the prospects for introduction of systems theoretical techniques in large capital projects within the above industries.

Peer-review under responsibility of the organizing committee of STAMP EU 2015

Keywords: STAMP; systems theoretic safety; process safety

1. Introduction

Over the past several decades the concept of process safety has become the norm for energy & chemicals Operating Companies (OPCOs), being variously required by legislation as well as company and industry standards and practices. In the past twenty years or so these industry safety standards have been migrating to performance based requirements rather than the traditional prescriptive codes. However the energy industry still adheres to several tried and tested safety codes, as mandated by the various authorities having jurisdiction. A prime example is the protection of steam boilers (e.g., NFPA® 85 Boiler and Combustion Systems Hazards Code).

In energy & chemicals industry operations throughout much of the world, process safety can be summarized as comprising:

- A fairly substantial documentation of hazardous processes (e.g., HAZID - hazard identification, SRS - Safety Requirements Specification)

* Corresponding author. Tel.: +01-403-537-4975; fax: +01-403-537-4222.
E-mail address: Stephen.Johnson@fluor.com

Peer-review under responsibility of the organizing committee of STAMP EU 2015
doi:10.1016/j.proeng.2015.11.506

- Some composite of quantitative and/or qualitative risk analysis (e.g., LOPA - layers of protection analysis, FTA - fault tree analysis, Risk Matrix evaluation, SIL - safety integrity level design verification)
- Some attempt to address system interactions (e.g., systematic capability as per IEC61508 “Functional safety of electrical/electronic/programmable electronic safety-related systems”, process alarm overload of the human operator as per ANSI/ISA 18.2 “Management of Alarm Systems in the Process Industries”)
- Some means to manage changes in design and their implications (e.g. MOC - management of change process).
- Some means to validate continued reliability of operation by implementing an appropriate maintenance and testing regime (e.g., device proof testing method sheets).

The backdrop to this view of process safety has been the implementation of increasingly complex software driven automation strategies in the energy industries brought about by the incredible advances in smart measurement technologies, computer processing power and development of more sophisticated control algorithms. The trend has been to push the envelope of plant optimization closer to the safety design margins and human capacity to oversee.

Many of the systems to analyze process safety predate these rapid changes in the way plants are controlled (e.g., HAZOP was first developed by ICI UK PLC in the mid-1960s). As the control of process plants has increased in complexity additional techniques have been used to supplement the original process safety analyses (e.g., LOPA, FMEA - failure mode and effects analysis, Risk Matrix). This has culminated in the acceptance of various international performance standards (e.g., IEC 61511 Functional safety — Safety instrumented systems for the process industry sector) which emphasize the concept of the Safety Life Cycle.

The use of performance based process safety techniques is potentially an improvement from no such requirements. However, while these performance standards do make an attempt to control “systematic” errors they do not provide rigorous methodologies for achieving this goal. It is also worth noting that many, but by no means all, industrialized nations have some kind of process safety regulations – for example, the EU, UK, Norway, & USA do, whereas Canada & Japan largely do not. These regulations provide some framework to reduce workforce injuries and mortality, but are neither adequate nor necessary to provide an adequately safe hydrocarbon extraction industry. Most major operating companies (OPCOs) already implement such frameworks globally, but the smaller companies may have little to no real risk management programs beyond what the regulators require them to implement.

Nomenclature

ANSI	American National Standards Institute
Bowtie	A semi-quantitative risk methodology
EO	Ethylene Oxide
FMEA	Failure Mode and Effects Analysis
HAZID	Hazard Identification
HAZOP	Hazard and Operability Study
HSE	Health, Safety & Environment
IEC	International Electrotechnical Commission
ISA	International Society for Automation
LOPA	Layers of Protection Analysis, a semi-quantitative risk methodology
NFPA	National Fire Protection Association
OPCO	Operating Company
PHA	Process Hazard Analysis

1.1. Process safety in the energy & chemicals world

Hazard & Operability reviews (HAZOP) and other forms of Process Hazard Analysis (PHA) have been an integral part of the design verification of process plants for several decades. These ubiquitous tools have been used in their various forms for everything from large scale multi-billion dollar projects through to periodic plant safety analyses

and to validating the integrity of minor plant modifications. As with many human endeavors, these design verification processes have been born in response to disasters involving significant plant damage and worse still, loss of life.

The application of PHA and related techniques to Process Plant designs is almost a reflex action. It is always seen as a critical milestone on the project schedule. The PHA implementation project bulletin is a key document painstakingly developed by the HSE & Process disciplines. A fundamental purpose of HAZOP and other formal safety reviews is Hazard Identification. If possible and warranted by the available information hazard evaluation is also an important outcome. The final outcome of the Hazard Identification process is the design of safeguards that are appropriate for the risk as determined by hazard evaluation (i.e. risk ranking).

At a stage when the design is more complete there are "predictive, analytical methods that have as their common denominator the incident scenario," [1]. These scenario-based procedures include:

- What-If Analysis
- What-lf/Checklist Analysis
- Hazard and Operability (HAZOP) Studies
- Failure Modes and Effects Analysis (FMEA)
- Fault Tree Analysis (FTA)
- Event Tree Analysis (ETA)
- Cause-Consequence Analysis (CCA) and Bow-Tie Analysis

From a classical execution viewpoint, it should be noted that the final HAZOP and/or What-If reviews should be conducted as formal audits, or verification, of essentially complete designs [2]. In this framework a HAZOP does not stand on its own but relies on the overall design process to properly consider hazards, risks and safeguards. A common next step is to carry out a Layers of Protection Analysis (LOPA) which uses the concept of "independent protection layers" to guard against hazards. Identified safeguards are mixture of procedural, mechanical, process design and instrumented systems. There are rules to determine independence of the various layers and some effort is taken to address impediments to proper human operator actions.

As an example ANSI/ISA 18.2 "Management of Alarm Systems in the Process Industries" provides a basis for designing a process alarm system that can help the operator rather than be overwhelming. However, the details are executed, the safeguarding result is a somewhat linear scheme which does not inherently control to the safety constraints. One result is that each group looking after a safety function does not always know the interaction with other safety functions (see process incident example below).

1.2. Process safety design example – Ethylene Oxide

Fig. 1 is a greatly simplified ethylene oxide reactor, which is used to produce varying grades of surfactants. Ethylene oxide is slowly injected, to a pre-determined total, into an autoclave which has been preloaded with catalysts and/or reagents. The reaction is very strongly exothermic. It relies on controlling the injection rate to maintain the heat output within the cooling capacity of the autoclave. Some of the safeguarding barriers are:

- High pressure control override of the flow injection
- High- high temperature shut-off of the flow injection
- High-high pressure shut-off of the flow injection
- Mechanical over pressure protection (i.e. relief valve to flare)

It should be noted that the flow totalizing controls are regarded in the process industries as a potential hazard initiator, not a safeguard (i.e. the failure of the flow injection totalizer may cause of the hazard). The safeguards are inert unless a process limit is reached. Proof testing is therefore required to validate that they remain operational.

Other important safeguards not shown in Fig. 1 relate to back flow protection. If the reaction pressure rises to be higher than the ethylene oxide injection system there is a risk of back flow of reaction materials into the feed line. This will result in an uncontrolled reaction outside the autoclave leading to potential explosion. Ethylene oxide (EO)

is a very reactive material with both short term toxic and long term carcinogenic effects. The material is normally kept refrigerated. If trapped in piping between blocked valves it can expand very significantly leading to very high pressures and release via flange leaks. Liquid thermal reliefs have to be carefully designed taking note of the health effects if released to atmosphere. Plant operations and maintenance personnel are acutely aware of the issues with ethylene oxide and are trained to take adequate precautions when dealing with the product.

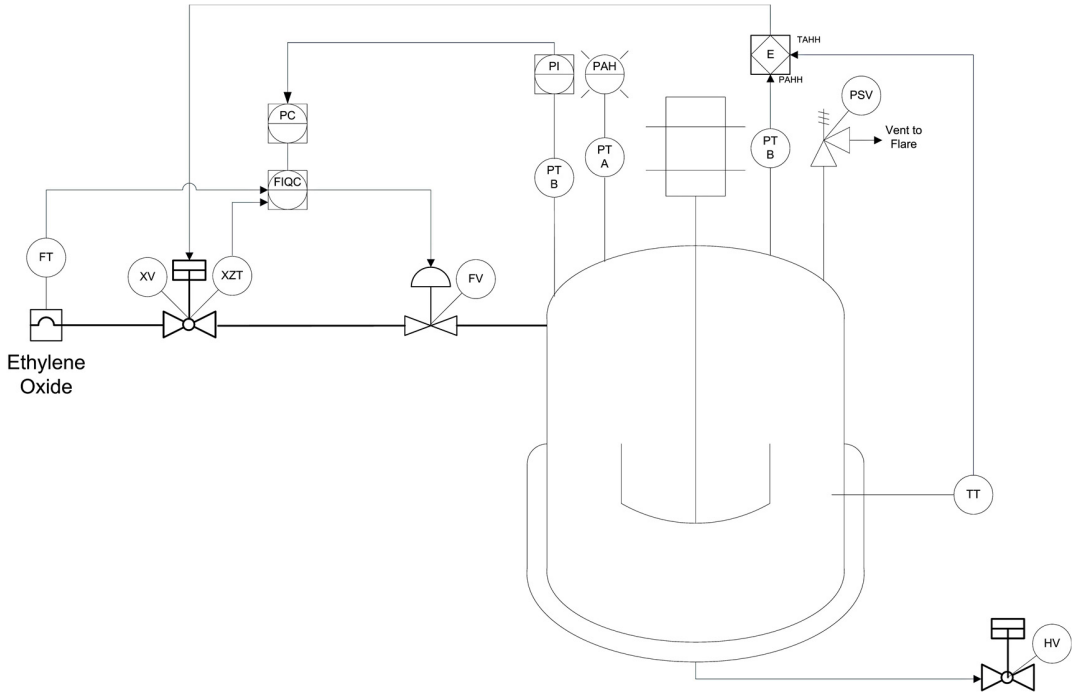

Fig. 1. Ethylene oxide reactor

1.3. Process Safety Incident

During a normal reaction cycle involving the autoclave in Fig. 1 mechanical maintenance personnel noticed that the trip valve XV was leaking slightly around the body stem packing. Understanding the consequences of EO release to atmosphere they sought to remedy the problem by tightening the stem packing. Since this fixed the immediate problem, nobody thought that there were further issues to resolve (or to report). The complete reaction could take up to 12 hours. It was not until much later when the safeguarding system needed to act on a high-high pressure trip that the real hazard was revealed. Since the stem packing was over tightened from the previous impromptu maintenance the XV stuck open; the actuator now did not have enough spring force to close the valve.

This should not have posed a problem since the control valve FV is also programmed to close on trip conditions. However, the normal program cycle was to close the XV first and to close the FV sometime later in order for the last part of the feed line to be completely empty (i.e. avoid thermal expansion of trapped EO). This program action was accomplished by interlocking the FV closure to the position of the XV (i.e. via XZT position measurement). Since the trip valve was stuck open the FV was kept open (i.e. system failure). Fortunately, the control room operator was able to note the failure of the controls and take corrective action to prevent a potentially hazardous event.

The reactor controls and safeguards had been recently upgraded from a largely local panel controls to a remote fully automatic batch controls together with a programmable safeguarding system. This allows for operators to be located away from the potential plant hazards. The design of the automation systems was subject to intensive scrutiny

(HAZOP, Control HAZOP; CHAZOP, reliability analysis). The programming update to the control system was easily worked out after the event. However, the incident provides evidence on how the complexities of modern automation schemes can camouflage faults.

This incident happened nearly twenty years ago and the authors are now starting to reflect on how system engineering may have viewed this incident. One obvious systems theoretic lesson is that hazards are not the result of a linear chain of events. There are many different risks associated with the control of EO; some competing for attention. There is a web of interactions that need to be controlled. This may involve additional people than are involved in traditional hazard identification exercises

2. Careful expert thought

There is no substitute for careful expert thought; providing that thought, however, is easy to say, but hard to do. Some barriers to the kind of careful, expert thought which is needed for effective systems theoretic implementation that we will address in this paper are:

- Constraints on time and expertise
- Risk and the problem of scale
- The countervailing effect of engineering sophistication

A few more obstacles not further detailed in the paper also include:

- Lack of regulatory or public pressure
- An industry which is reluctant to change
- A collective mental model heavily invested in blaming operations personnel errors and/or equipment failure

2.1. Time and expertise in short supply

There was a time when most of the major OPCOs had significant internal expert groups who could be engaged for the resolution of more complex problems. To a large degree these groups have been eliminated, and now the situation is that fairly inexpert users are trying to apply complex - and often performance or risk based - standards that they understand fairly poorly. Many of the OPCOs have elected to publish heavily prescriptive guidelines as a substitute, but while prescriptive standards can, in principle help significantly, they require a considerable level of expertise and care in development or review. The experience has been that - in most cases – the level of effort has been inadequate to the task. Finally, even the best standards cannot prevent blinkered and unthinking application by individuals who have only limited understanding of the intent behind them. All these problems are further exacerbated by the increasingly stringent constraints on project schedules and manpower.

2.2. Risk and the problem of scale

In general, the kinds of risk matrices used by many OPCOs have two fundamental problems:

- Risk perception is a function of organizational scale
- Risk matrices break down at the corners

The first point is simply a function of the mathematics of catastrophe – for a Tier 1 size Oil & Gas Company, sooner or later catastrophes will occur, but a brand new one-plant operating company may well perceive the kind of catastrophe that becomes a byword as simply vanishingly unlikely. Hence, smaller and newer OPCOs have less of an incentive to really evaluate their worst case scenarios carefully. The second reflects an intrinsic weakness of risk matrices – they perform poorly at the corners that reflect frequent-but-trivial and catastrophic-but-rare. More quantitative techniques – typically used much more extensively (and, as a rule, understood better) by larger

organizations are required to handle those. As a result, these two considerations tend to indicate that larger OPCOs are more likely to be the ones to see the potential benefits of the systems theoretic approach, absent some regulatory requirement.

2.3. The countervailing effect of engineering sophistication

While it might seem from the previous paragraph that the most sophisticated OPCOs may be the best customers for a Systems theoretic implementation, there is a significant countervail – these OPCOs are the one with robust technical safety groups, well-developed guidance and expectations that an adequately executed program consistent with their approach can yield a satisfactory level of facility risk. As a result, they may, surprisingly, have less incentive to adopt new approaches.

3. Traditional process safety activities and systems theoretic world

Clearly, extant tools, like Systems Theoretic Process Analysis (STPA), System-Theoretic Early Concept Analysis (STECA) and Causal Accident Systems Theoretic (CAST) models are available for use [3], but the focus here is on already accepted tools that might be effectively applied in a manner consistent with systems theoretic thought.

3.1. General Safety Systems Engineering

The concept of the sociotechnical web is shown in Fig. 2 [4]. So, the analytical framework already present can be expanded into other areas. The downside is that few engineering personnel get involved with this kind of analysis at all, and it's largely specialists with advanced analytic skills. However, it is a valuable starting point for moving into the more complex world of systems theoretic analysis, and particularly towards the understanding that high software/system reliability is neither necessary nor sufficient for safety - though in the hydrocarbon processing world high reliability will likely continue to be viewed as essential for some time.

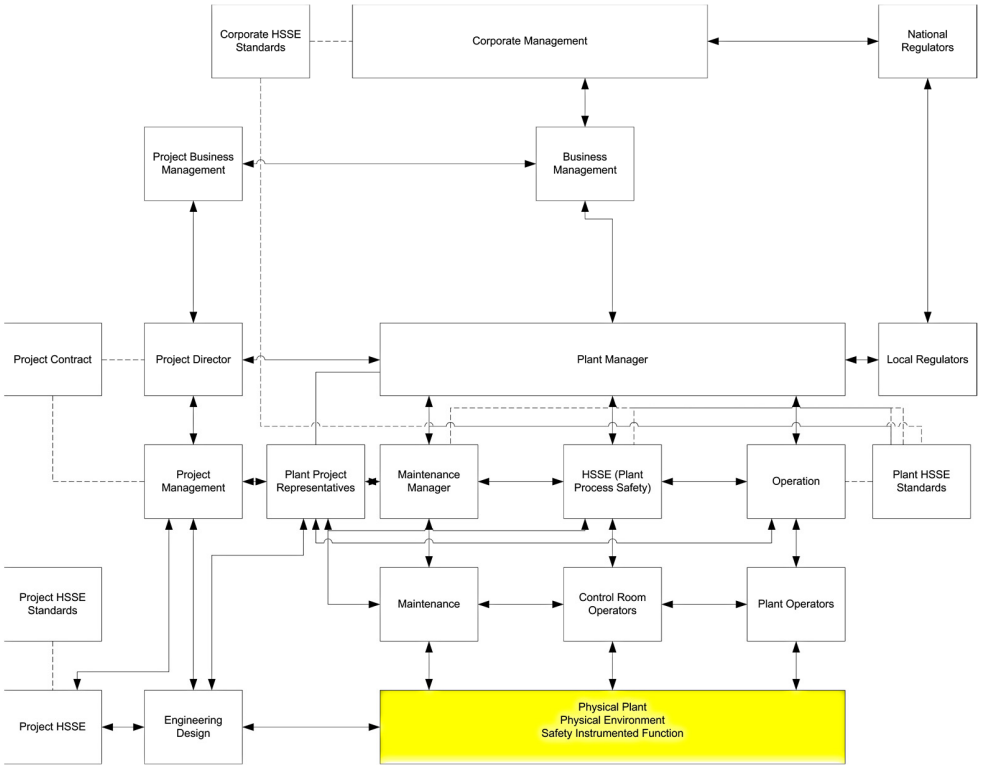

Fig. 2. The sociotechnical web in process safety

3.2. Opportunities in semi-quantitative techniques

Another technique that has struck the authors as potentially useful is the semi-quantitative Layers of Protection Analysis (LOPA) and Bow-tie approaches. While the objection could be made that chain-of-events narratives – which these methods certainly are – are not the best tool for conveying how untoward events may occur, these techniques combine relative simplicity with a reasonably meaningful level of analysis, taking the user away from the always problematic issue of risk perception that one sees in qualitative reviews such as PHA towards a more scientific model of risk, which we believe can be a logical halfway house for reaching the systems constraint and complex causality approach that is the ultimate transition objective. Broadly stated, our thesis for this specific item is that transitioning users from LOPA to a more bowtie centric approach can help them to see the complex sociotechnical web that underlies most accidents in a more gradual manner.

Table 1. LOPA versus Bowtie

LOPA	Bowtie
Semi-quantitative	Semi-quantitative
Single cause	Multiple causes are possible
Single end result	Multiple end results
Quite widely accepted	More narrow acceptance
Easy to understand	More complex to understand

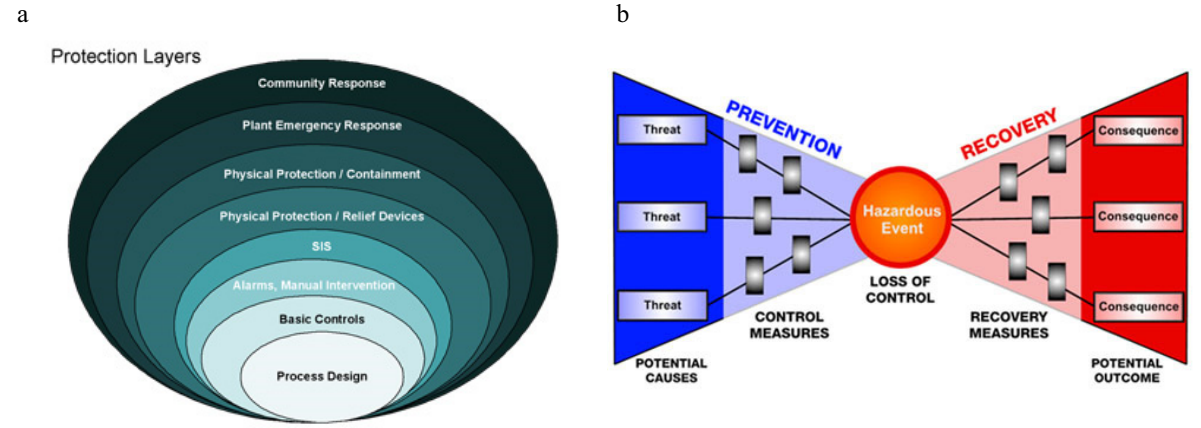

Fig. 3. (a) LOPA; (b) Bowtie

3.3. Alarm proliferation

Sophisticated plant automation systems have become readily available, and increasingly affordable. The down side of this is that the number of instruments and alarm points proliferates to the point that malfunctions within the control system start to become a significant fraction of the cause for incidents, and in the event of a significant upset, alarm floods can simply overwhelm the operations personnel. It is no longer unusual for projects to add instruments and alarms in the PHA (it's easy, and feels like it might be useful), followed by their subsequent removal in the alarm rationalization. This is a clear indication that many people involved in the design simply do not really understand the implications of their actions. In the process incident described above the operator was able to respond to the alarms and take appropriate action - ANS/ISA 18.2 is a tool that seeks to address the problematic designs that lead to "alarm flooding" and the resulting confusion in the control room. This process leads itself to integration into the system engineering approach.

4. Design safety in the energy & chemicals industry

There are features specific to the hydrocarbons project world, which make it a little different from, (for example) nuclear, military, medical and aerospace analyses.

4.1. Reliability concepts are not going away soon – or easily

One of the most important reasons is that - to a first approximation - all process safety failures in our industry involve not just one component failure, but usually multiple ones, and that loss of containment is usually at the center of the multi-casualty incidents that make up our textbook cases. As a result, we believe that reliability, availability and other statistical models are often still the best available tools for risk elimination at the present, especially given the limited expertise of many of the audience. Also, many regulators now require such analyses as a pre-condition of operation, convincing them to accept STPA and similar techniques will likely take some time.

4.2. The capital projects limitation

Engineering, procurement, fabrication and construction companies (EPC), as a rule, do not own or operate facilities. As a result, they often have limited ability to prevent the system as designed from migrating to a state of higher risk after their involvement ends. They can advise clients in the strongest of terms not to depart from the safe design criteria provided to them, but once a project is complete, EPC companies have no effective control over how the OPCOs run their new facilities.

5. Conclusions

Notwithstanding the adverse factors described above, it's not really bad news, though progress is typically driven by the pace of organizational change, rather than technological possibility. The authors believe that the kind of statistical techniques used in process safety do represent a significant advance on opinion as a guide to managing risk. With time and patience, we believe that we can insert more rigorous and all-encompassing technologies, such as the systems theoretic framework. Furthermore, these more rigorous techniques should provide a much more structured means for the OPCOs to operate their facilities within the operating constraints identified in the design.

References

[1] CCPS, Guidelines for Hazard Evaluation Procedures, third ed., Wiley, 2008.
[2] D. P. Nolan, Application of HAZOP and What-If Safety Reviews to the Petroleum, Petrochemical and Chemical Industries, Noyes Publications, Jersey, 1994.
[3] N.G. Leveson, Engineering A Safer World: Systems Thinking Applied to Safety, MIT Press, Cambridge, MA, 2011.
[4] S. Lucchini, Back To The Future: Why Are We Doing This HAZOP?, Mary K O'Connor Process Safety Center International Symposium 2012, Texas, 2012.